UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF RHODE ISLAND

UNITED STATES OF AMERICA	)	
	)	
vs.	)	CR No. 11-082S
	)	
DONALD J. JONES, III a/k/a Don Juan	)	

GOVERNMENT'S TRIAL MEMORANDUM

I. INTRODUCTION

On December 22, 2011, a federal grand jury returned a six-count Superseding Indictment charging the Defendant, Donald J. Jones, III, a/k/a Don Juan, with one count of Aggravated Sexual Abuse, in violation of Title 18 United States Code, Section 2241(c); one count of Coercion and Enticement of a minor in violation of Title 18 United States Code, Section 2422(b); one count of Travel with Intent to engage in illicit sexual conduct with a person under the age of 18 years old, in violation of Title 18 United States Code, Sections 2423(b) and (f); one count of transportation of child pornography, in violation of Title 18 United States Code, Sections 2252(a)(1) and (b)(1); one count of possession of child pornography, in violation of Title 18 United States Code, Sections 2252(a)(4)(B) and (b)(2); and one count of the commission of a felony by a person required to register as a sex offender, in violation of Title 18 United States Code, Section 2260A. The case is scheduled for trial on May 14, 2012. The government expects that its case-in-chief will last seven days.

II. SUMMARY OF THE GOVERNMENT'S EVIDENCE

The Government expects the evidence at trial to establish the following facts regarding the conduct charged: on March 19, 2011, a person using the email address

donjuan045@gmail.com, created a profile on the Internet website "Motherless.com" using the user name "donjuan045" with the title "the younger the better."[1] After the title, the following ad was posted "Looking for white mothers and fathers who have young and would like to see their daughters get parted by a normal to moderate black sized pole." The user also wrote that he was "wanting a real life meeting." The photo associated with the profile for donjuan045 was of a young girl, approximately 4 to 6 years old, who appears to be grasping a male penis with ejaculate on the child's face. Donjuan045 joined a group on Motherless.com on March 19, 2011 called "Very Cute Only." A posting on the home page for "Very Cute Only" posted the following question, "Tell us what is the youngest you will fuck??" Donjuan045 posted an answer "i wont go below 5 not a definite but a fairbase line."[2]

On March 21, 2011 a United States Postal Service Inspector working in an undercover capacity responded to the above post, using the screen name, "attila1." The undercover agent

[1] A response to an administrative subpoena from Motherless.com indicated that the subscriber registered from email donjones045@gmail.com, which Defendant admitted in a statement to Detective Fitzpatrick upon his arrest was his email account (Defendant's Statement "Def. St." lines 421- 443). The Motherless.com response also noted that the Internet Protocol ("IP") address that was used to create the account and profile was 69.171.167.72, an IP assigned to a New Jersey location, where the Defendant resided.

[2] The government is waiting for additional information from Google Inc., and has made an additional application with this Court for a 2703(d) court order to obtain further details to corroborate and identify the Defendant as the participant in eight on-line chats discussing his sexual interest in young girls. Although the gmail subscriber logs authenticate the IP address to the Defendant in several of the chats, some information regarding the exact IP address of four of the chats is incomplete. However, the Motherless.com posting, which was identified by the Defendant's IP address, uses the same language in the chats the United States is seeking to admit. For example, "the younger the better," and "tired of looking want real" is contained in the email chats the United States is seeking to admit, and indicative that the Defendant is the person involved in the internet chats. The government also may be able to corroborate through defendant's other email accounts that the Defendant was on-line at the time he engaged in the chats. If, at the time of trial, the government does not have the necessary evidence to authenticate the gmail on-line chats, it will not seek to have the evidence admitted.

told donjuan045 that he had an eight-year-old daughter and maybe the two of them could work something out. The Defendant and the undercover officer, known to him as "Jim," then communicated through a private on-line chat, one that is not public to other individuals on the website or in the chat room, for approximately two days. During the course of their on-line chats, the Defendant expressed interest in meeting Jim's daughter and suggested "a hotel up ur way." Donjuan045 also asked Jim, "will I get a chance to touch her or just look at her . . . I would be so gentle and kind to her and would come bearing gifts." On March 24, 2011, donjuan045 gave his cell phone number, (609)845-5723 and private email address (not connected through Motherless.com), donjuan045@gmail.com to "Jim." They continued to communicate by email and telephone. Many of the telephone calls were taped. The Defendant, over the course of a few weeks, sent emails with attachments containing child pornography and links to rapidshare.com (a file-hosting site that allows for longer videos) containing child pornography to Jim. The attachments and links were videos exclusively of prepubescent females ranging in age from approximately six months old to approximately six years-old. In the videos, the children were shown engaging in oral sex, vaginal intercourse and other acts with adult males. Further, the telephone calls and emails document the Defendant's purchase of an outfit from a children's clothing store that he sent by express mail to Jim to give to his daughter. Telephone calls and emails also document the Defendant's plans for his trip to Rhode Island. The Defendant made bus reservations and a hotel reservation at La Quinta Hotel in Warwick, Rhode Island. On April 8, 2011, the Defendant traveled by bus from Philadelphia, Pennsylvania to Providence, Rhode Island. He was arrested upon his arrival at Kennedy Plaza.

Upon his arrest, Defendant was carrying a Dell laptop computer, a thumb drive, and two cell phones. The thumb drive was examined by a computer forensics expert from the Internet

Crimes Against Children Task Force, Robert Fitzpatrick and Britnee Morgan from the Rhode Island State Police. Analysis of the thumb drive yielded evidence of approximately 110 images and 33 videos of child pornography. Many of the videos and images on the thumb drive were downloaded onto the thumb drive on April 7, 2011, the day before his trip to Rhode Island. Many of the names assigned to these image files were indicative of child pornography such as "6yo Tiny Tessa (3) Taking a Dick in the Ass 2008.wmv." The thumb drive also contained the Defendant's resume and a cover letter applying for a job. The cell phone analysis revealed several images of child pornography. In addition, forensic analysis and comparison of the video attachments sent by donjuan045@gmail.com to the undercover agent and the videos contained on the thumb drive revealed matching hash values (a "digital thumbprint") for seven of the videos.

Copies of the images were sent to the National Center for Missing and Exploited Children ("NCMEC") for analysis. The NCMEC collects images of child pornography that were created using known victims. Different images of the same victim are referred to as a series. NCMEC keeps information about the victim and the law enforcement officer who investigated the original case. Upon request, NCMEC compares images of child pornography recovered during criminal investigations with those in its collection and determines whether any match and therefore can identify known victims. NCMEC reported several of the videos and images obtained from the Defendant's thumb drive and from emails that he sent to the undercover agent matched images of known victims in its collection. The known victims are all from other states and countries. The laptop computer was encrypted, and could not be analyzed. The cell phone data contained several video images of child pornography, a note in the calendar for the

Greyhound Bus information for the trip to Rhode Island, and the phone number for Jim saved in his contacts.

On April 8, 2011, a search warrant issued by the United States District Court for the District of New Jersey was executed at 245 Washington Street in Mount Holly, New Jersey, one of the places where the Defendant was living in New Jersey. The Defendant's nephew also lived at that address, in an upstairs bedroom. In a makeshift bedroom used by the Defendant, agents found still images of child pornography inside an envelope, that was mixed in with miscellaneous papers like utility and telephone bills addressed to the Defendant. Handwritten notes on a Direct TV bill with the Defendant's address included the file name of a child pornography video "Tessa," that he sent Jim, and discussed in several calls with Jim. The still images on the cell phone include images of prepubescent girls. An Acer Aspire One Netbook computer was also recovered from 245 Washington Street with the user name "donjuan," and contained evidence of child pornography.[1] Although the Defendant lived with his nephew at 245 Washington Street, forensic analysis of the Acer computer established that the Defendant had control and possession of the computer. The forensic analyst observed several files with references to email accounts owned by the Defendant including donjones3rd@hotmail.com, donjonesiii@yahoo.com, and donaldjonesiii@lycos.com. The computer also contained a resume of the Defendant and several images of the Defendant. The examination contained over 150 images of child pornography. These images depict prepubescent females, including infants, engaged in sexual acts, including bondage. Further, the forensic examiner observed links to a

[1] Although the Acer notebook computer has been in the evidence room, which defense counsel has been invited to view since the inception of the case, the government just recently performed a forensic analysis on the computer and provided it to defense counsel the date it was received. Although the Acer analysis was made relatively recently, the possession of these images do not form the substance of either the possession or transportation of child pornography. However, they are relevant to show that the defendant acted knowingly in possessing the images, and the possession of the Acer laptop computer at his home also confirms that the possession is not the result of some outside source, such as a virus, or another person who used his gmail account, which is one of the anticipated defenses at trial.

LimeWire folder containing images and video file names that are consistent with child pornography. The images were deleted and unable to be recovered. Analysis also revealed access to several websites related to child pornography and Yahoo searches for "lolita pedo" and "hussyfan." The Defendant waived his Miranda rights and agreed to be interviewed. Defendant admitted that he had traveled from Pennsylvania that morning. In Defendant's statement to Detective Robert Fitzpatrick, he said, in part, that he was simply traveling to Rhode Island to meet Jim, because he could not believe that he would allow him access to his eight year old child and he "wanted to see what played out. Because I didn't believe it for a second." (Def. Stmt. lines 60-62, provided separately to the Court April 17, 2012) Defendant also stated that he sent Jim images but that he did not know that they contained child pornography, he never opened the files, he just forwarded them to Jim. He further stated that another person had access to his gmail account, and that the other person may have sent attachments and other contraband to Jim. Because of the potential defenses in this case, particularly lack of intent, identification, admission (i.e. another person had access to the gmail account), and his denial of looking at the attachments containing child pornography, evidence regarding the Defendant's prior convictions and intent in this case are essential and material to the charges.

III. ANALYSIS OF THE APPLICABLE LAW

Below is a summary of the elements of the offenses detailed above.

A. Aggravated Sexual Abuse

Count One of the Superseding Indictment charges the Defendant with Aggravated Sexual Abuse: Crossing a State Line with the Intent to Engage in a Sexual Act with a Child Under The Age of 12. The elements of the offense are that: (1) the Defendant crossed a state line, (2) with the intent to engage in a "sexual act" (as defined in 18 U.S.C. § 2246(2)) with a person who had

not attained the age of 12 years. The government need not prove that the Defendant knew that the other person engaging in the sexual act was under the age of twelve years. See United States v. Felton, Slip Copy, 2011 WL 1362298 (D. Ak. April 11, 2011).

Title 18 U.S.C. § 2246(2) defines "sexual act" as: (A) contact between the penis and the vulva or the penis and the anus, and for purposes of this subparagraph contact involving the penis occurs upon penetration, however, slight; (B) contact between the mouth and the penis, the mouth and the vulva, or the mouth and the anus; (C) the penetration, however slight, of the anal or genital opening of another by a hand or finger or by any object, with an intent to abuse, humiliate, harass, degrade, or arouse or gratify the sexual desire of any person; or (D) the intentional touching, not through the clothing, of the genitalia of another person who has not attained the age of 16 years with an intent to abuse, humiliate, harass, degrade, or arouse or gratify the sexual desire of any person.

There is no requirement that the government must show actual sexual contact in Count One. If a defendant travels in interstate commerce with the requisite intent to engage in a sexual act with a child under the age of twelve, and takes a substantial step towards committing the crime, that is sufficient. The "sexual act" does not need to have been completed in order to find the defendant guilty of the charge. See 18 U.S.C. § 2241(c); United States v. Felton, Slip Copy, 2011 WL 1362298 (D. Ak. April 11, 2011).

The Internet is considered a facility or means of interstate commerce. See United States v. Carroll, 105 F.3d 740, 742 (1st Cir. 1997).

B. Coercion and Enticement of A Minor

Count Two charges the Defendant with Coercion and Enticement of a Minor. The elements of the offense of Coercion and Enticement of a Minor are: (1) that the Defendant used

a facility or means of interstate commerce, that is, the Internet or the mail, (2) to attempt to, or to knowingly, persuade, induce, or entice, (3) someone younger than eighteen years old, (4) to engage in criminal sexual activity. See United States v. Brand, 467 F.3d 179, 201-202 (2d Cir. 2006).

The offense does not require proof of an intent to engage in the sexual activity. See United States v. Dwinells, 508 F.3d 63, 65 (1st Cir. 2007). Section 2422(b) "was designed to protect children from the act of solicitation itself," United States v. Hughes, 632 F.3d 956, 961 (6th Cir. 2011), and it "criminalizes an intentional attempt to achieve a mental state – a minor's assent – regardless of the accused's intentions [concerning] the actual consummation of sexual activities with the minor." United States v. Berk, 652 F.3d 132, 140 (1st Cir.2011). Although "it may be rare for there to be a separation between the intent to persuade and the follow-up intent to perform the act after persuasion, they are two clearly separate and different intents and the Congress has made a clear choice [in § 2422(b)] to criminalize persuasion and the attempt to persuade, not the performance of the sexual acts themselves." United States v. Bailey, 228 F.3d 637, 639 (6th Cir.2000); see also, United States v. Hofus, 598 F.3d 1171, 7778 (9th Cir. 2010) (Section 2422(b) "requires an attempt to persuade, induce, entice, or coerce a minor to engage in criminal sexual activity. . . . There is a difference in attempting to persuade, induce, entice or coerce a minor to *engage* in sexual activity and actually *attempting to engage* in sexual activity with the minor" (emphasis added).

The Defendant can be found guilty of attempted enticement even though the person he seeks to entice does not exist. See e.g. United States v. Root, 296 F.3d 1222, 1227 (11th Cir. 2002). Attempted enticement may also be accomplished through an adult intermediary, such as the minor's parent or guardian. See United States v. Murrell, 368 F.3d 1283 (11th Cir. 2004).

The government does not have to prove the presence of an actual minor for a prosecution pursuant to 18 U.S.C. §§ 2241(c), 2422(b) or 2423(b). See, e.g., United States v. Kelly, 510 F.3d 433 (4th Cir. 2007).

As a matter of Rhode Island law, sexual activity, including sexual contact, sexual penetration, and sexual intercourse with a person under the age of 14 years is a criminal offense. See R.I. Gen.Laws 1956, § 11-37-1; § 11-37-8.1; § 11-37-8.3; see also, United States v. Dwinells, 508 F.3d 63, 72 (1st Cir. 2007). The government will request Judicial Notice of Rhode Island law in the jury instructions, and provide the Court with the public documents noting Rhode Island law with a seal pursuant to Federal Rule of Evidence 201.

C. Traveling in Interstate Commerce For the Purpose of Engaging in Illicit Sexual Conduct

Count Three charges the Defendant with traveling in interstate commerce for the purpose of engaging in "illicit sexual conduct." The elements of that offense are: (1) that the Defendant traveled in interstate commerce, and (2) the Defendant's purpose in traveling in interstate commerce was to engage in illicit sexual conduct with a person under the age of 18 years. For this charge, a person travels in interstate commerce when he travels from one state to another state.

This offense is completed when the Defendant travels across state lines with the purpose of engaging in illicit sexual contact. The person with whom the Defendant intended to engage in a sexual act does not need to be an actual minor in order for the Defendant to be guilty of the charge. The government need only prove that the Defendant believed that the person was a minor.

In addition, the sexual act does not need to have been completed in order to find the Defendant guilty of the charge. Moreover, the ability to successfully complete the sexual act is

immaterial. It is not a defense to the charge that, as a result of circumstances unknown to the Defendant, he was unable to complete the intended sexual act or acts. Similarly, it is not a defense to the charge that the person with whom the Defendant intended to engage in the sexual act was not, in fact, a minor, so long as the Defendant believed that a person existed and was under the age of 18. United States v. Aigbevbolle, 827 F.2d 664 (10 Cir. 1987); United States v. Kufrovich, 997 F. Supp. 246, 257 (D. Conn. 1997).

The statute defines "illicit sexual conduct" as a "sexual act," as defined above, with a person under the age of 18 years, that would be a violation of any of the sexual offenses set forth in chapter 109A. See 18 U.S.C. § 2423(f) 18, 18 U.S.C. § 2246.

D. Transportation of Child Pornography

Count Four charges the Defendant with transportation of child pornography. The elements of that offense are: (1) that the Defendant knowingly distributed a visual depiction in interstate commerce by any means, including by computer; (2) that the production of such visual depiction involve[d] the use of a minor engaging in sexually explicit conduct; (3) that such visual depiction is of such sexually explicit conduct; that the visual depiction of the minor is of a real child; and that the Defendant knew that such visual depiction was of a minor engaged in sexually explicit conduct. See 18 U.S.C. § 2252(a)(1) and Ninth Circuit Model Jury Instruction 8.153.

An act is done "knowingly" if it is done voluntarily and intentionally, and not because of mistake or accident.

An image constitutes "child pornography" within the meaning of the statute if it depicts a minor engaging in "sexually explicit conduct." 18 U.S.C. § 2256(8)(A). A "minor" is a child under the age of 18 years. 18 U.S.C. § 2256(1). "Sexually explicit conduct" includes actual or simulated sexual intercourse, bestiality, masturbation, sadistic or masochistic abuse, or lascivious

display of the genitals or pubic area of a person. 18 U.S.C. § 2256(2). To determine if an image constitutes a "lascivious display" within the meaning of the statute, the Court may, but is not required to, consider six factors: (1) Whether the genitals or pubic area are the focal point of the image; (2) Whether the setting of the image is sexually suggestive (i.e., a location generally associated with sexual activity); (3) Whether the child is depicted in an unnatural pose or inappropriate attire considering his or her age; (4) Whether the child is fully or partially clothed, or nude; (5) Whether the images suggest sexual coyness or willingness to engage in sexual activity; and (6) Whether the image is intended or designed to elicit a sexual response in the viewer. United States v. Amirault, 173 F.3d 28, 31 (1st Cir. 1999); First Circuit Pattern Jury Instructions § 4.18.2252.

The term "visual depiction" includes undeveloped film and videotape, and data that has been stored on a computer disk or thumb drive, or data that has been stored by electronic means and that is capable of conversion into a visual image. For example, a video, still image, or photograph containing child pornography would satisfy the definition. See 18 U.S.C. §2256(5).

The government is not required to prove that the Defendant knew the precise contents of the images transported or possessed, or knew that the pictures were illegal under federal law. Rather, it must only be shown that he knew the images were child pornography. See United States v. Brown, 862 F.2d 1033, 1037-38 (3d Cir. 1988). The government must prove that the image depicts an actual, real child. United States v. Hoey, 508 F.3d 687, 691 (1st Cir. 2007); United States v. Hilton, 386 F.3d 13, 18 (1st Cir. 2004). A defendant's knowledge may be shown by direct or circumstantial evidence, or both. Eyewitness testimony of the defendant's receipt or viewing of images or videos of child pornography is not necessary to prove his awareness of its contents; the circumstances may warrant the inference that he was

aware of what the material depicted. Furthermore, the defendant's belief as to the legality or illegality of the material is not controlling. See United States v. X-Citement Video, Inc., 513 U.S. 64 (1994). In the absence of direct evidence to the contrary, the government is not required to introduce expert testimony that the children depicted in the images are actual children. See United States v. Rodriguez-Pacheco, 475 F.3d 434, 440-41 (1st Cir. 2007); United States v. Hoey, 508 F.3d at 691. The fact finder is permitted to make that determination from the images alone. Rodriguez-Pacheco, 475 F.3d at 441. However, due to the mandatory life sentence enhancement under 18 U.S.C. § 2241(c), the government, in an abundance of caution, will call an expert to verify that the images are real and not digitally manufactured. Recent dicta FIRST CIRCUIT REAL CHILD CASE indicates that it is best practice to call an expert.

E. Possession of Child Pornography

Count Five charges the Defendant with Possession of Child Pornography. The elements of that offense are: (1) the knowing possession of a computer, computer disc, thumb drive or hard drive storage device; (2) and that the computer, computer disc, or thumb drive or other storage device contained at least one image of child pornography; (3) that the Defendant knew that the computer, computer disc, or hard drive storage device contained an image of child pornography; and (4) that the image of child pornography had been transported in interstate or foreign commerce by any means including by computer or the internet, or was produced using materials that had been transported in interstate or foreign commerce by any means, including by computer or the internet. See Judge D. Brock Hornby's 2012 Revisions to Pattern Criminal Jury Instructions for the District Courts of the First Circuit § 4.18.2252 (12/23/2010 D. Me. internet site ed.).

To satisfy the interstate or foreign commerce element of the offense, the government may prove that the visual depictions were transmitted over the Internet. See United States v. Lewis, 554 F.3d 208, 215 (1st Cir. 2009); First Circuit Pattern Instructions § 4.18.2252.2. Circumstantial evidence may be used to establish this fact. See, e.g., United States v. Dodds, 347 F.3d 893, 900 (11th Cir. 2003).

An alternative method of satisfying the interstate commerce element is to prove that the child pornography was produced using materials that moved in interstate commerce. See First Circuit Pattern Instructions § 4.18.2252 n.9. For example, utilization of computer disks manufactured overseas or a thumb drive manufactured overseas to copy or download images of child pornography satisfies this jurisdictional element. See United States v. Anderson, 280 F.3d 1121, 1123 (7th Cir. 2002); United States v. Guagliardo, 278 F.3d 868, 870-71 (9th Cir. 2002). An image is "produced" when it is copied using computer equipment that has traveled in interstate commerce. United States v. Angle, 234 F.3d 326, 341 (7th Cir. 2000), cert. denied, 533 U.S. 932 (2001); see also, United States v. Schene, 543 F. 3d 627 (10th Cir. 2008).

F. Felony Offense Involving A Minor

The Defendant is charged in Count Six of the Superseding Indictment with The Commission of a Felony Offense Involving A Minor by an Individual Required to Register as a Sex Offender. The elements for the charge are: (1) that the Defendant committed a felony offense involving a minor; and (2) that at the time he committed the felony offense involving a minor, the Defendant was required by Federal or other law to register as a sex offender. Title 18 U.S.C. Section 2260A clearly delineates sections 2241, 2242 or 2423 (Counts One, Two and Three charged in the Superseding Indictment) as felony offenses involving a minor.

A defendant is required to register under the Sex Offender Registration and Notification Act if he is a "sex offender" under federal or other law. A "sex offender" is a person who has been convicted of a qualifying "sex offense." The Defendant's conviction of Aggravated Sexual Abuse in New Jersey Superior Court in 1993, requires him to register as a sex offender for fifteen years from the date of release. The government will submit documentation of a certified copy of the Judgment of Conviction and a certified copy of the Complaint filed in the 1993 case, including the requirement to register as evidence that the Defendant is required to register as a sex offender under the National Sex Offender Registry, which can be located on a public web site at http:// www. nsopr. gov, and will ask the Court to take judicial notice that the Defendant was required to register as a sex offender on the date of offense in this case.

IV. EVIDENTIARY ISSUES AND MATTERS TO BE RESOLVED PRIOR TO TRIAL

There are several evidentiary issues which, among others, the Court may wish to address prior to trial. As to two of issues, the government has separately filed two *motions in limine* with the Court on April 17, 2012, requesting a pre-trial ruling on the admissibility of certified business records without the requirement of the testimony of a custodian of records, and the admissibility of evidence pursuant to Federal Rules of Evidence 414 and 404(b), including Defendant's three prior convictions for child molestation offenses in New Jersey Superior Court and eight emails and chats, from donjuan045@gmail.com to persons other than the undercover agent, as evidence of his intent.

A. Electronic Evidence - Overview

At trial, the government will offer electronic evidence obtained during the course of the investigation. The electronic evidence includes e-mails, subscriber log files, Internet history

files, records, business records, videos, images, and photographs. As set forth below, courts have held that this evidence is admissible under the Federal Rules of Evidence. As with other evidence, e-mails, log files, photographs, attachments, images, user history, and other records obtained from the seized computers and thumb drive are admissible where the requirements of the Federal Rules of Evidence are satisfied.[2]

1. Authentication

The foundational "requirement of authentication or identification as a condition precedent to admissibility is satisfied by evidence sufficient to support a finding that the matter in question is what its proponent claims." Fed. R. Evid. 901(a).[3] Rule 901(a) only requires the government to make a prima facie showing of authenticity or identification "so that a reasonable juror could find in favor of authenticity or identification."[4] Once the threshold showing has been met to admit the document, any questions concerning the genuineness of the item normally go to the weight of the evidence.[5]

Through a number of established means, electronic evidence will be authenticated in this

[2] The m*otion in limine* regarding Self-Authenticating Business Records Under FRE 902(11) analysis also applies to the electronic evidence in this case. The government maintains that the data compilation and information provided pursuant to administrative subpoenas to Google, Yahoo, Hotmail, and other Internet Service Providers in this case fall squarely within the definition of Self-Authenticating Business Records. Again, the government filed a separate *motion in limine* on this issue.

[3] See also United States v. Dhinsa, 243 F.3d 635, 658-59 (2d Cir. 2001) (noting Rule 901 "does not erect a particularly high hurdle," and that hurdle may be cleared by "circumstantial evidence") (quoting United States v. Ortiz, 966 F.2d 707, 716 (1st Cir. 1992).

[4] United States v. Chu Kong Yin, 935 F.2d 990, 996 (9th Cir. 1991), cert. denied, 511 U.S. 1035 (1994); see also Lexington Ins. Co. v. Western Pennsylvania Hosp., 423 F.3d 318, 328-29 (3d Cir. 2005) ("Once a prima facie case is made, the evidence goes to the jury and it is the jury who will ultimately determine the authenticity of the evidence, not the court. The only requirement is that there has been substantial evidence from which they could infer that the document was authentic.").

[5] Orr v. Bank of America, 285 F.3d 764, 773 n.6 (9th Cir. 2002) ("Once the trial judge determines that there is prima facie evidence of genuineness, the evidence is admitted, and the trier of fact makes its own determination of the evidence's authenticity and weight."); United States v. Paulino, 13 F.3d 20, 23 (1st Cir. 1994) ("In respect to matters of authentication, the trial court serves a gatekeeping function. If the court discerns enough support in the record to warrant a reasonable person in determining that the evidence is what it purports to be, then Rule 901(a) is satisfied and the weight to be given to the evidence is left to the jury").

case, as noted below:

a. By Witness With Knowledge

As with other records, e-mails and other records may be authenticated under Fed. R. Evid. 901(b) by a witness with knowledge. For example, this permits authentication by a witness who participated in the e-mail communications. See, e.g., United States v. Gagliardi, 506 F.3d 140, 151 (2d Cir. 2007) (in prosecution for attempting to entice a minor to engage in prohibited sexual activity, e-mails and chat room communications between the defendant and a private citizen informant and undercover agent were authenticated by the informant and agent who "testified that the exhibits were in fact accurate records of Gagliardi's conversations with" persons he knew as "Lorie" and "Julie"; fact that the e-mails and transcripts of instant-message chats were imported into another document, were not originals and could have been edited did not prevent admission; "a reasonable juror could have found that the exhibits did represent those conversations, notwithstanding that the e-mails and online chats were editable"); United States v. Tank, 200 F.3d 627, 630 (9th Cir. 2000) (prima facie showing of authenticity established concerning chat room log printouts; witness "explained how he created the logs with his computer and stated that the printouts, which did not contain the deleted material, appeared to be an accurate representation of the chat room conversations among members of the Orchid Club"); see also United States v. Safavian, 435 F.Supp.2d 36, 40 n.2 (D.D.C. 2006) (noting e-mails between defendant government official and lobbyist could have been authenticated by recipient and sender but government chose not to call the lobbyist during trial).

b. By Agent

An agent familiar with the process used to obtain the e-mails and other records from the seized computers will assist in authenticating these records in this case. For example, a forensic

agent will testify about the process used to obtain the computer records from the seized computers. See, e.g., United States v. Whitaker, 127 F.3d 595, 601 (7th Cir. 1997) (in conspiracy to distribute marijuana case, a computer seized from one defendant's residence contained computer records of drug transactions and the drug business; rejecting argument that government was required to supply a witness with personal knowledge of the computer system; agent testimony authenticated the computer printouts under Rule 901(a) including that the computer was seized during the execution of a warrant, the agent was present when the computer records "were retrieved from the computer using the Microsoft Money program," and the agent "testified concerning his personal knowledge and his personal participation in obtaining the printouts"). The government may use "chain of custody" testimony to establish how the government obtained items located on the defendant's Acer computer and thumb drive. See, e.g., United States v. Salcido, 506 F.3d 729, 733 (9th Cir. 2007) (per curiam) (in prosecution involving the possession and receipt or distribution of material involving the sexual exploitation of minors, "the government properly authenticated the videos and images under Rule 901 by presenting detailed evidence as to the chain of custody, specifically how the images were retrieved from the defendant's computers").

An undercover agent may also assist in authenticating communications obtained during an undercover investigation. See, e.g., United States v. Simpson, 152 F.3d 1241, 1249-50 (10th Cir. 1998) (the defendant claimed the government could not show the defendant had conversed with an undercover FBI agent in a chat room devoted to child pornography; the agent testified about his Internet chat conversation with an individual identified as 'Stavron' who also gave the undercover agent his name and used an e-mail address which belonged to the defendant).

c. By Distinctive Characteristics

Under Fed. R. Evid. 901(b)(4), authentication may be made by distinctive characteristics, which may include "[a]ppearance, contents, substance, internal patterns, or other distinctive characteristics, taken in conjunction with circumstances." Courts have relied upon this rule in admitting e-mail and chat communications bearing distinctive characteristics. For example, this may include the e-mail addresses used in the communications, the context and circumstances, and other surrounding circumstances. See, e.g., United States v. Siddiqui, 235 F.3d 1318, 1322 (11th Cir. 2000) (in fraud, false statements, and obstruction case, e-mail authenticated by contents and context, including e-mail address, automatic reply to sender, the messages indicated knowledge of matter, and use of nicknames; and foreign deposition testimony concerning phone conversations after e-mail messages were transmitted, applying Rule 901(b)(4)), cert. denied, 533 U.S. 940 (2001); United States v. Safavian, 435 F.Supp.2d at 40 (e-mails between defendant government official and lobbyist were authenticated by distinctive characteristics under Rule 901(b)(4) including the e-mail addresses used which bore the sender's and recipient's names; "the name of the sender or recipient in the bodies of the e-mail, in the signature blocks at the end of the e-mail, in the 'To:' and 'From:' headings, and by signature of the sender"; and the contents).

A "hash value" or hash algorithm provides another accepted method to authenticate an electronic document by distinctive means.[6] In this case, hash values were obtained as part of the

[6] Hash value is defined as:

"A unique numerical identifier that can be assigned to a file, a group of files, or a portion of a file, based on a standard mathematical algorithm applied to the characteristics of the data set. The most commonly used algorithms, known as MD5 and SHA, will generate numerical values so distinctive that the chance that any two data sets will have the same hash value, no matter how similar they appear, is less than one in one billion. 'Hashing' is used to guarantee the authenticity of an original data set and can be used as a digital equivalent of the Bates stamp used in paper document production."

forensic examination process. A computer forensics expert will testify how these measurements were made during the forensic examination process and the significance of these measurements. Courts have used "hash values" as one means of authenticating electronic evidence. See, e.g., Lorraine v. Markel American Ins. Co., 241 F.R.D. 534, 546-47 (D. Md. 2007) ("Hash values can be inserted into original electronic documents when they are created to provide them with distinctive characteristics that will permit their authentication under Rule 901(b)(4)."); Williams v. Sprint/United Mgmt. Co., 230 F.R.D. 640, 655 (D. Kan. 2005) (hash value "allows a large amount of data to be self-authenticating with a rather small hash mark, efficiently assuring that the original image has not been manipulated").

d. By Comparison

Under Fed. R. Evid. 901(b)(3), authentication may be made by either the trier of fact or an expert." Under this rule, the jury, as the trier of fact, may compare authenticated specimens with the evidence sought for admission. Some courts have used this rule to authenticate e-mails. See, e.g., United States v. Safavian, 435 F.Supp.2d at 40-41 (e-mails between defendant government official and lobbyist were authenticated by comparing e-mail addresses, the use of the defendant's name and business). In this case, there are some e-mails which may be authenticated or are readily subject to authentication. The government will use these authenticated e-mails to authenticate other evidence obtained in the case.

2. Hearsay Issues

Some of the electronic evidence exhibits (including e-mails and other records) contain non-hearsay since the information is not offered to prove the truth of the matter asserted or does not meet the definition of hearsay under Fed. R. Evid. 801(c). For example, machine-generated

---

Federal Judicial Center, Managing Discovery of Electronic Information: A Pocket Guide for Judges, Federal Judicial Center, 2007 at 24 (quoted in Lorraine v. Markel American Ins. Co., 241 F.R.D. at 546-47 & n.23.).

information does not raise any hearsay issues. The statements contained in the e-mail, and other records obtained from the seized computer are admissible based on (1) non-hearsay purposes; (2) party-opponent statements; and (3) statements which satisfy an established hearsay exception.

a. Non-Hearsay

Statements introduced for a non-hearsay purpose do not violate the hearsay rule. See, e.g., Anderson v. United States, 417 U.S. 211, 219 (1974) ("Out of court statements constitute hearsay only when offered in evidence to prove the truth of the matter asserted."); United States v. Jaramillo-Suarez, 950 F.2d 1378, 1383 (9th Cir. 1991) (noting that where the probative value of a document "was independent of the truth of its contents, the rule against hearsay was not implicated"; pay-owe sheets introduced for the non-hearsay purpose to show the character of the place not for the truth of the statements).

i. Machine-Generated Information

Some of the evidence at trial will include machine-generated information. For example, this includes the IP address, logs, date and time, screen name, file path and sender information on e-mails. The courts have consistently held that machine-generated information is not hearsay as no "person" is making a statement. See, e.g., United States v. Hamilton, 413 F.3d 1138, 1142-43 (10th Cir. 2005) (computer-generated "header" information (including the screen name, subject of the posting, the date the images were posted, and the individual's IP address) was not hearsay; no "person" acting as a declarant).[7]

[7] See also United States v. Washington, 498 F.3d 225, 231 (4th Cir. 2007) (in DUI case, machine-generated data used to determine whether a blood sample contained drugs or alcohol were not statements of the lab technicians and were not hearsay statements, since they were not made by persons but machines analyzing the sample; no Confrontation Clause issues); United States v. Khorozian, 333 F.3d 498, 506 (3d Cir.) (information automatically generated by fax machine is not hearsay since "nothing 'said' by a machine . . . is hearsay"), cert. denied, 540 U.S. 968 (2003).

ii. Supplying Context

As noted below, the statements of the defendant on e-mails are directly admissible against the defendant under Fed. R. Evid. 801(d)(2)(A). The statements of others used in the e-mails and chat communications are admitted not for the truth of the matter but as non-hearsay to supply context. See, e.g., United States v. Burt, 495 F.3d 733, 738-39 (7th Cir.) (in prosecution for sexual exploitation of a minor, distributing child pornography, and possession of child pornography, in Yahoo! chat communication involving the defendant and a third party found on the defendant's computer, the portion from the third party was admissible as non-hearsay and provided context to the conversation; "The government had no reason to prove the particular sexual activities that [third party] Martin engaged in with particular boys whose photos he might have been sharing with [defendant] Burt."), cert. denied, 128 S.Ct. 724 (2007); United States v. Dupre, 462 F.3d 131, 136-37 (2d Cir. 2006) (in wire fraud prosecution, e-mails from investors demanding information about defendant's fraudulent scheme were not hearsay when offered not for truth of the assertion that the scheme was fraudulent, but to provide context for the defendant's message sent in response and to rebut defendant's argument that she did not know scheme was fraudulent; no Confrontation Clause issues arose since the statements were offered for a non-hearsay purpose); Safavian, 435 F.Supp.2d at 44 (admitting some e-mails which "provide context for the defendant's statements and are not introduced for their truth").

iii. Establishing Relationship and Custom of Communicating

The e-mail and records seized from the computer are also admissible for the non-hearsay purpose to show the relationship of the parties and their custom in communicating. See, e.g., Siddiqui, 235 F.3d at 1322 ("Those [e-mails] sent by Siddiqui constitute admissions of a party pursuant to Fed. R. Evid. 801(d)(2)(A), and those between Siddiqui and Yamada unrelated to the

NSF investigation are non-hearsay admitted to show Siddiqui's and Yamada's relationship and custom of communicating by e-mail."); Safavian, 435 F.Supp.2d at 44 (e-mails were admissible for the non-hearsay purpose to show the lobbying "work" between lobbyist and government official; "It is the fact of these discussions rather than the contents (or the truth or accuracy thereof), that is being offered by the government on the theory that the e-mails themselves actually are Mr. Abramoff's lobbying 'work' and 'business.'"). In this case, several e-mails will be offered to show the relationship of Defendant to the undercover, and his communication with others with whom he used his email address "donjones045@gmail.com."

b. Hearsay Exceptions

In addition to the foregoing reasons, some of the computer records obtained in this case are admissible under well-recognized hearsay exceptions. This includes as: (1) business records; and (2) public records, as set forth in the separate *motion in limine*.

i. Computer Business Records

Business records are admissible as an exception to the rule against hearsay. Fed. R. Evid. 803(6). See, e.g., United States v. Baker, 693 F.2d 183, 188 (D.C. Cir. 1982) ("The justification for this exception is that business records have a high degree of accuracy because the nation's business demands it, because the records are customarily checked for correctness, and because recordkeepers are trained in habits of precision."). A business record is admissible where a record "must (1) have been prepared in the normal course of business; (2) . . . have been made at or near the time of the events it records; and (3) . . . be based on the personal knowledge of the entrant or of an informant who had a business duty to transmit the information to the entrant." Hertz v. Luzenac America, Inc., 370 F.3d 1014, 1017 (10th Cir. 2004) (admitting INS computer printout concerning amnesty application).

The business records rule expressly applies to a "memorandum, report, record, or *data compilation*, in any form." (Emphasis added.) The terms "data compilation" are "used as broadly descriptive of any means of storing information other than the conventional words and figures in written or documentary form. It includes, but is by no means limited to, electronic computer storage." Fed. R. Evid. 803(6) Advisory Committee Notes.

It is well-settled that records generated by a computer are admissible under Fed. R. Evid. 803(6). In essence, "it is immaterial that the business record is maintained in a computer rather than in company books." United States v. Catabran, 836 F.2d 453, 457 (9th Cir. 1988) (computer used to create ledger) (citation and internal quotation marks omitted). There are many examples where computer business records were admitted under Rule 803(6).[8]

B. Expert Testimony

A witness who is "qualified as an expert by knowledge, skill and experience" may present expert testimony if his or her specialized knowledge will assist the trier of fact to understand the evidence or to determine a fact in issue. Fed.R.Evid. 702. The admission of expert testimony is a matter within the sound discretion of the trial court. Under Federal Rule of Evidence 702, Britnee Morgan, a certified computer forensic examiner, a Forensic Analyst for the Rhode Island Internet Crimes Against Children Task Force, is expected to testify about the results of her forensic examinations of the Acer laptop computer seized from Defendant's residence pursuant to a search warrant at 245 Washington Street in New Jersey and the items Defendant possessed upon his arrest including a thumb drive, both of which contained images

[8] See, e.g., Sea-Land Service, Inc., v. Lozen Intern., LLC., 285 F.3d 808, 819-20 (9th Cir. 2002) (bills of lading); United States v. Salgado, 250 F.3d 438, 452 (6th Cir.) (telephone toll records); Dyno Const. Co. v. McWane, Inc., 198 F.3d 567, 576 (6th Cir. 1999) (Federal Express delivery records); United States v. Cestnik, 36 F.3d 904, 909-10 (10th Cir. 1994) (money transfer orders); United States v. Loney, 959 F.2d 1332, 1341-42 (5th Cir. 1992) (frequent flier airline miles admitted under Rule 803(6) and Rule 1006); United States v. Moore, 923 F.2d 910, 914 (1st Cir. 1991) (loan histories); United States v. Miller, 771 F.2d 1219, 1237 (9th Cir. 1985) (computer-generated toll and billing records).

and videos of child pornography. Analyst Morgan will also testify about the technology and steps that she took to perform her analysis in this case, including EnCase. The EnCase program is well known and is a generally accepted means of conducting a forensic examination of a computer for the purpose of retrieving evidence. Considering the fact that defense experts commonly rely upon the same program, the government anticipates no objection to the use of EnCase in the present investigation. See, e.g., Sanders v. State, 191 S.W.3d 272, 277 (Tex.App.-Waco, 2006) ("EnCase is a 'field standard' for forensic computer examination; treatises about EnCase have been published."). She will also testify about the results of her examination of Defendant's gmail accounts, computers, and thumb drive. A copy of her forensic reports, and all of the data she retrieved from Defendant's computers, storage devices and emails has been provided in discovery and the tangible evidence has been available for inspection.

Detective Robert Fitzpatrick, a certified computer forensic examiner employed by the Rhode Island Police Department and assigned to the Rhode Island Internet Crimes Against Children Task Force is expected to testify about the technology and steps that he took to perform the analysis in this case, including using EnCase. A copy of all data he retrieved from Defendant's Acer computer, storage devices, cell phones, and email accounts, has been provided in discovery or made available for inspection. Detective Fitzpatrick will explain to the jury the process he used to identify the Defendant through various means, including use of Defendant's internet protocol address, e-mail addresses, screen names and online identities; evidence of remote or offsite file storage locations (physical or virtual); subscriber log information; typical nomenclature practices followed by consumers and distributors of child pornography; the incriminating purpose of otherwise legitimate software applications, and encryption of hard

drives, and what the significance of encryption typically means in the child pornography community, chat rooms and their general operation; Internet Service Providers, their general operation, what information they provide, such as subscriber information, message headers and content; File Sharing and File hosting websites; Peer to Peer software; the "interstate commerce" aspect of the internet; chat rooms including an explanation of the motherless.com website and chat room; various methods the Defendant used to upload, download, distribute, transport and possess child pornography, including evidence that child pornography files were viewed, uploaded, played, downloaded, unzipped, or saved, metadata and the significance of various image and video files; identified images and videos of child pornography on the defendant's media, including the thumb drive and cell phone, all as summarized in government's evidence previously disclosed to the defense.

The Government further intends to call Computer Forensic Specialist Richard Kaplan as an Expert Witness, from the Child Exploitation and Obscenity Section, High Technology Investigative Unit ("HTIU") at the Department of Justice in Washington D.C. He examined the Dell laptop computer, which was encrypted in this case, and also did a forensic analysis of the cell phones and thumb drive and will testify about his findings. A copy of his forensic reports has been provided in discovery, and the tangible items have been made available for inspection.

Finally, the government intends to elicit testimony from an expert witness, Hany Farid, in the field of digital imaging technology. Mr. Farid is a professor at Dartmouth College, and has been qualified as an expert and testified in federal court three times, most recently in a child pornography case in the District of Massachusetts, before United States District Judge F. Dennis Saylor, IV, in the case of United States v. Paul Burdulis in April, 2012. Dr. Farid will review the files, and based on that review, we expect that the expert will testify that the images and videos,

in fact, depict real children. Again, although the law does not require an expert to testify, the government expects that the testimony will help the jury understand the sophisticated and rapidly expanding technology available in the area of digital imaging.

C. Defendant's Statements

The government anticipates introducing statements made by the defendant during the interview after his arrest on April 8, 2011, in e-mails, in chats, and in telephone calls with the undercover agent. Under the Federal Rules of Evidence, a defendant's statement is admissible only if offered against him. Fed.R.Evid.801(d)(2)(A) (a statement is not hearsay if . . . (2) Admission by party-opponent. The statement is offered against a party and is (A) the party's own statement, in either an individual or a representative capacity ....). The government may introduce statements of the defendant to third persons under Federal Rule of Evidence 801(d)(2). With regard to statements made prior to or contemporaneous with the crimes charged, corroboration is not required. Smith v. United States, 348 U.S. 147, 154 (1954).

D. Audiotapes and Transcripts

The government intends to introduce taped conversations of phone calls between the Defendant and undercover agent. The government may also introduce the taped statement of the Defendant, made after he waived his Miranda rights, to Detective Fitzpatrick and Special Agent Donaghy. The transcripts and CDs were provided to the Court on April 17, 2012. The government provided an additional bound courtesy copy to the defense counsel, but he has had the materials since August 2011. All that is required to authenticate such recordings is "proof that the . . . recording[s] accurately reflect[] the conversation in question." United States v. Doyon, 194 F.3d 207, 212 (1st Cir. 1999). The Court has wide discretion to permit jurors to have transcripts of recordings. United States v. Rengifo, 789 F.2d 975, 980 (1st Cir. 1986). However,

the words that the jurors hear are the evidence, not the words that they read in the transcript. The government does not intend to play the entire transcripts, but only excerpts of specific conversations and statements, which will be cued to the correct place in the recordings, to make the introduction of the evidence as efficient as possible.

E. Presentation of Child Pornography Evidence

The government intends to offer a limited, representative sample of still image files, video files, and screen captures containing child pornography. Some of the images are very graphic. Given the very high burden of proof generally, and that the government will need to prove the defendant acted intentionally and knowingly in committing all charged offenses, the government should be given wide latitude in deciding what is an appropriate number of images to be introduced into evidence. Since the government's burden is extremely high, the government should "not be restricted to a modest quantum of evidence that will support the indictment." United States v. Gallo, 543 F.2d 361, 365 (D.C. Cir. 1976).

Depending on the type of evidence (e.g. image file or video file), the government plans to offer evidence containing child pornography in a printed format placed in binders and/or through the Court's audio/visual system. The government intends to offer image files by printing color copies of the image files and placing them in a binder. Prior to trial, the defense will be permitted to review the binder. One binder will be marked as containing the original trial exhibits. A copy of the binder will be provided to the Court, defense counsel, and each member of the jury. After the binder is admitted and discussed at trial, the binders for the Court, defense counsel, and each member of the jury can be placed under seal in the Court's vault. During jury deliberations, the binder marked as containing the original trial exhibits can be provided to the jury in the jury room, upon their request. The government anticipates introducing image files, video files, and screen captures into evidence through the Court's audio/visual system.

While it is standard practice for most exhibits to be displayed on the screen for public view, the government requests that exhibits containing child pornography not be displayed for public view, but rather be published only to the monitors at the bench, witness stand, counsel table, and the jury chairs, but not to the public monitors. The government also requests that the monitors be angled or positioned so that display of the evidence is limited with regard to onlookers.

Furthermore, the government does not intend, during its case-in-chief, on playing any of the offered videos in their entirety. Only a sample portion of the videos will be published in open court. However, after laying the proper foundation, the complete videos will be offered into evidence by the government. The government proposes that should the jury want to review the videos in their entirety, that during jury deliberations, the videos can be played in the jury room on a DVD player upon their request.

F. Summaries of Evidence

The Government may offer into evidence exhibits which summarize other documentary evidence or testimony. Rule 1006 of the Federal Rules of Evidence provides for the admission of such summaries. United States v. Johnson, 54 F.3d 1150, 1158 (4th Cir. 1995) (summary charts may summarize documents and/or the testimony of witnesses or documents); United States v. Goldberg, 401 F.2d 644, 647 (2d Cir. 1968) (same).

Summarized documents do not have to be admitted into evidence, but must constitute admissible evidence, and be available for examination and copying by the defense and production in court, if so ordered. See Fed. R. Evid. 1006; United States v. Conlin, 551 F.2d 534, 538 (2d Cir. 1977). In accordance with this Rule, courts have routinely allowed the Government to introduce charts and summaries based on the evidence. United States v. Nivica,

887 F.2d 1110, 1125 (1st Cir. 1989); United States v. Drougas, 748 F.2d 8, 25-26 (1st Cir. 1984). Such summaries may be provided to the jury for its use during deliberation. Holland v. United States, 348 U.S. 121, 128 (1954); United States v. Pinto, 850 F.2d 927, 935 (2d Cir. 1988).

CONCLUSION

This trial brief has covered matters which the Government believes will be of assistance to the Court. The Government requests leave of Court to file other such memoranda of law as may be necessary or appropriate.

Respectfully submitted,

UNITED STATES OF AMERICA
By its Attorneys,

PETER F. NERONHA
United States Attorney

/s/ STEPHEN G. DAMBRUCH
STEPHEN G. DAMBRUCH
Assistant U.S. Attorney

/s/ LESLIE J. KANE
LESLIE J. KANE
Assistant U.S. Attorney
United States Attorney's Office
Email Stephen.dambruch@usdoj.gov
Email Leslie.kane@usdoj.gov

CERTIFICATE OF SERVICE

On this 24th day of April, 2012, I caused the within Government's Trial Brief to be filed electronically and it is available for viewing and downloading from the ECF system.

Electronic Notification:

Charles A. Tamuleviz, Esquire
Darrow Everett, LLP
One Turks Head Place
Suite 1200
Providence, RI 02903
email: ctamuleviz@darroweverett.com

/s/ STEPHEN G. DAMBRUCH
STEPHEN G. DAMBRUCH
Assistant U.S. Attorney

/s/ LESLIE J. KANE
LESLIE J. KANE
Assistant U.S. Attorney
U.S. Attorney's Office
50 Kennedy Plaza, 8th FL
Providence, RI 02903
Tel (401) 709-5049
Fax (401) 709-5001
email stephen.dambruch@usdoj.gov
email leslie.kane@usdoj.gov